IN THE UNITED STATES DISTRICT COURT

FOR THE EASTERN DISTRICT OF PENNSYLVANIA

IN THE MATTER OF THE SEARCH OF A BLACK SAMSUNG CELLULAR PHONE IMEI NO. 355357110651085 CURRENTLY IN THE CUSTODY OF THE FBI	**Magistrate No. 20-1862**

AFFIDAVIT IN SUPPORT OF AN APPLICATION UNDER RULE 41 FOR WARRANT TO SEARCH AND SEIZE

I, James Finnegan, being first duly sworn, hereby depose and state as follows:

INTRODUCTION AND AGENT BACKGROUND

1. I make this affidavit in support of an application under Rule 41 of the Federal Rules of Criminal Procedure for a warrant to search a black Samsung Cellular Telephone, serial number IMEI No. 355357110651085 (the "Device") in law enforcement possession at 600 Arch Street, Philadelphia, Pennsylvania, as further described in Attachment A, and the extraction from that property of electronically stored information described in Attachment B.

2. I have been employed by the Federal Bureau of Investigation for the last 14 years as a Special Agent. I am presently assigned to the Violent Crimes Task Force (VCTF) that investigates violations of state and federal laws, to include commercial robberies, bank robberies, kidnappings, fugitives, and major theft investigations of pharmaceutical drugs, among other violations of the law. I also have experience in the collection and examination of various forms of electronic evidence, including from cell phones. The statements in this affidavit are based on police reports, the recovery of physical evidence from the crime scene, and information provided

to me by law enforcement personnel and others. These statements are true and correct to the best of my knowledge, information, and belief.

3. This affidavit is intended to show only that there is probable cause for the requested warrants and does not set forth all of my knowledge about this matter.

PROBABLE CAUSE

4. On October 27, 2020, U.S. Magistrate Judge Richard A. Lloret approved a criminal complaint and arrest warrant charging Tricia Moon (also known as Trisha Moon and William Leinhauser)[1], with violating one count of 18 U.S.C. § 2113(a) (attempted bank robbery), for the September 24, 2020, attempted bank robbery of the Bank of America at 2118 Cottman Avenue, in Philadelphia, Pennsylvania.

5. On Thursday, September 24, 2020, at approximately 2:15 p.m., an unknown white person (the "Subject") entered the Bank of America located at 2118 Cottman Avenue, in Philadelphia, Pennsylvania (the "Bank of America"), approached the victim teller, and placed a piece of paper under the glass. The piece of paper had a note on it that stated:

---

[1] The government's understanding is Leinhauser has reported that her legal name is "Trisha Moon." However, records searches have not confirmed that Leinhauser has changed her legal name to Moon. Accordingly, the government will use and refer to Leinhauser by her currently known real name of "William Leinhauser." Further, Leinhauser recently reported that she identifies as a female using pronouns of she, her, and hers. But Leinhauser's records state she is a male and has presented to others as a male in the past. We endeavor to be respectful of Leinhauser's gender identity, and refer to Leinhauser's previously reported gender of a male only for clarity, and throughout this affidavit refer to Leinhauser by her preferred pronouns of "she" or "her." Finally, the government charged Leinhauser by criminal complaint as "Tricia Moon," but given a lack of confirmation that is her real name, further charging is likely to be in the name "William Leinhauser."

> This is a robbery. No dye packs, no tracers! Place all the 100s 50s 20s and 10s in the envelope free of bands. Place this note in envelope pass to me Act natural 45 secs to comply" (sic).

6. The victim teller hesitated and asked the Subject how she could help. The Subject replied, "Give it to me now, or I will shoot you, count to 10, if not I'll shoot you." The Subject made that statement while putting her hands down near her waistband. The victim teller was frightened and while she thought about giving the Subject the money, instead the victim teller grabbed her cash drawer keys and ran to the back of the bank refusing. Consequently, the Subject received no money.

7. The Subject left the bank and fled on foot in an unknown direction. The Subject was described as a white male, 5'5"-5'7" in height, wearing a medical mask, red hat under a black hooded sweatshirt, and white latex gloves. A neck tattoo was prominent on the Subject.

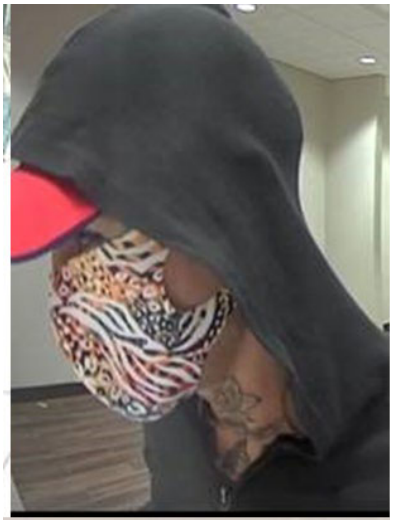
8. The deposits of the Bank of America located at 2118 Cottman Avenue in Philadelphia, Pennsylvania, are insured by the Federal Deposit Insurance Corporation (FDIC) and were insured by the FDIC at the time of the bank robbery described above.

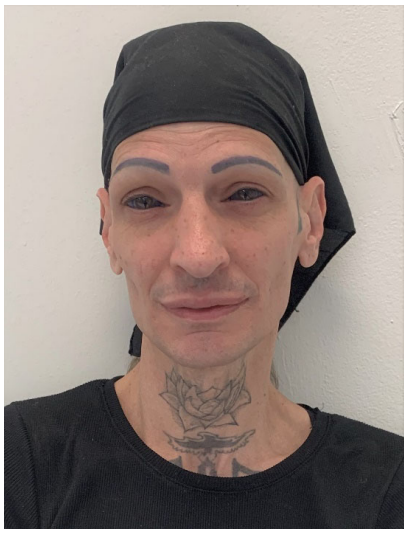
9. After the robbery, Philadelphia Police Department (PPD) Officers responded to the area. PPD conducted interviews, recovered the demand note and manila envelope left by the Subject, and collected surveillance video and photos. FBI VCTF issued a Wanted Flyer using the same surveillance photos.

10. On September 25, 2020, U.S. Probation Officer Carla Benjamin notified Special Agent Finnegan that she knew the Subject depicted in the Wanted Flyer for the robbery of Bank of America on September 24, 2020, as William Leinhauser, also known as Trisha Moon.

11. Officer Benjamin relayed she had been supervising Leinhauser since her release from federal prison on July 17, 2020. On two occasions, the U.S. District Court convicted and sentenced Leinhauser for bank robberies. Most recently, in Criminal No. 13-121, the Honorable Harvey Bartle, III sentenced Leinhauser to 84 months incarceration and 3 years' supervised release for a May 2014 robbery of a PNC Bank in Philadelphia. On November 19, 2007, in Criminal No. 06-631, the Honorable Paul S. Diamond sentenced Leinhauser to 77 months' imprisonment and 3 years' supervised release for robbing the same Commerce Bank in Philadelphia on two different occasions.

12. The following are two photos used by Officer Benjamin to identify Leinhauser as the person that attempted to rob the Bank of America on September 24, 2020. The photo on the left is a still photo from security surveillance footage from the attempted robbery of the Bank of America. The photo on the right is a known photo of Leinhauser.





13. On October 8, 2020, a forensic scientist with the Philadelphia Department of Forensic Science issued a report comparing Leinhauser known fingerprints to impressions on the

demand note and a manila envelope held by the Subject who attempted the September 24, 2020, bank robbery of Bank of America. The impressions on the manila envelope were individualized to Leinhauser's right ring finger and right little finger, respectively.

14. According to Officer Benjamin's records and discussions, on the date of the robbery, Leinhauser was living at 1002 Napfle Avenue, Apt. 2F, Philadelphia, PA 19111, which is only two miles away from the Bank of America.

15. On October 27, 2020, FBI investigators interviewed Leinhauser on the day of her arrest on the federal complaint and warrant for the robbery of the Bank of America. After providing Leinhauser her *Miranda* warnings, investigators interviewed Leinhauser. Initially, Leinhauser denied robbing the Bank of America on September 24, 2020. However, after being confronted with the photo of the Subject who robbed Bank of America, Leinhauser admitted that the person in the photo was her. Leinhauser stated she did not remember doing the attempted robbery due to her recent relapse of taking drugs, including K-2.[2]

16. As part of Leinhauser's arrest on October 27, 2020, the FBI investigators seized Leinhauser's phone, which is a black Samsung cellular telephone, IMEI No. 355357110651085 (the "Device"). This is the Device that is sought to be searched as described in Attachment A.

17. Based on my training and experience, in general the carrying of cell phones is almost ubiquitous.[3] Further, those committing criminal acts usually carry a cell phone to the

---

[2] K-2 is a synthetic version of tetrahydrocannabinol (THC), the psychoactive ingredient in marijuana. K-2 is often more potent than marijuana and can cause more deleterious side effects

[3] *See Carpenter v. United States*, 138 S.Ct. 2206, 2211 (2018) (stating that, as of

crime or keep one nearby. Even if a person has a cell phone, but does not carry that cell phone on him during the commission of a crime, the *inactivity* on the cell phone during the commission of a crime can constitute evidence of involvement in that crime. In the investigation of a bank robbery, a cell phone can be useful to research banks, research criminal strategy, communicate with others involved or aware of the bank robbery, route getaway options, check traffic, or listen to police scanners. Further, a cell phone often contains various forms of location data that can reveal where the user of a cell phone was located throughout a given day. A cell phone often also contains other records that can constitute evidence of a crime related to motive, opportunity, intent, preparation, plan, knowledge, identity, or absence of mistake.

18. The Device is currently in the lawful possession of the Federal Bureau of Investigation (FBI). It came into the FBI's possession as a seizure incident to arrest. I seek this warrant to be certain that an examination of the Device will comply with the Fourth Amendment and other applicable laws.

19. The Device is currently in storage at 600 Arch Street, Philadelphia, Pennsylvania. In my training and experience, I know that the Device has been stored in a manner in which its contents are, to the extent material to this investigation, in substantially the same state as they were when the Device first came into the possession of the FBI.

---

approximately June 2018, "there were 396 million cell phone service accounts in the United States—for a Nation of 326 million people"); *Riley v. California*, 572 U.S. 373, 395 (2014) (stating statistics show 90% of American adults own a cellular phone, and nearly three-quarters of smart phone users reported being within five feet of their phones most of the time). In Carpenter, the Court found that Americans have a "compulsive[]" need to carry and use their cellular phones. *Carpenter*, 138 S.Ct. at 2218 (citations omitted).

TECHNICAL TERMS

20. Based on my training and experience, I use the following technical terms to convey the following meanings:

a. Wireless telephone: A wireless telephone (or mobile telephone, or cellular telephone) is a handheld wireless device used for voice and data communication through radio signals. These telephones send signals through networks of transmitter/receivers, enabling communication with other wireless telephones or traditional "land line" telephones. A wireless telephone usually contains a "call log," which records the telephone number, date, and time of calls made to and from the phone. In addition to enabling voice communications, wireless telephones offer a broad range of capabilities. These capabilities include: storing names and phone numbers in electronic "address books;" sending, receiving, and storing text messages and e-mail; taking, sending, receiving, and storing still photographs and moving video; storing and playing back audio files; storing dates, appointments, and other information on personal calendars; and accessing and downloading information from the Internet. Wireless telephones may also include global positioning system ("GPS") technology for determining the location of the device.

b. Digital camera: A digital camera is a camera that records pictures as digital picture files, rather than by using photographic film. Digital cameras use a variety of fixed and removable storage media to store their recorded images. Images can usually be retrieved by connecting the camera to a computer or by

connecting the removable storage medium to a separate reader. Removable storage media include various types of flash memory cards or miniature hard drives. Most digital cameras also include a screen for viewing the stored images. This storage media can contain any digital data, including data unrelated to photographs or videos.

c. Portable media player: A portable media player (or "MP3 Player" or iPod) is a handheld digital storage device designed primarily to store and play audio, video, or photographic files. However, a portable media player can also store other digital data. Some portable media players can use removable storage media. Removable storage media include various types of flash memory cards or miniature hard drives. This removable storage media can also store any digital data. Depending on the model, a portable media player may have the ability to store very large amounts of electronic data and may offer additional features such as a calendar, contact list, clock, or games.

d. GPS: A GPS navigation device uses the Global Positioning System to display its current location. It often contains records the locations where it has been. Some GPS navigation devices can give a user driving or walking directions to another location. These devices can contain records of the addresses or locations involved in such navigation. The Global Positioning System (generally abbreviated "GPS") consists of 24 NAVSTAR satellites orbiting the Earth. Each satellite contains an extremely accurate clock. Each satellite repeatedly transmits by radio a mathematical representation of the current time, combined with a special

sequence of numbers. These signals are sent by radio, using specifications that are publicly available. A GPS antenna on Earth can receive those signals. When a GPS antenna receives signals from at least four satellites, a computer connected to that antenna can mathematically calculate the antenna's latitude, longitude, and sometimes altitude with a high level of precision.

e. PDA: A personal digital assistant, or PDA, is a handheld electronic device used for storing data (such as names, addresses, appointments or notes) and utilizing computer programs. Some PDAs also function as wireless communication devices and are used to access the Internet and send and receive e-mail. PDAs usually include a memory card or other removable storage media for storing data and a keyboard and/or touch screen for entering data. Removable storage media include various types of flash memory cards or miniature hard drives. This removable storage media can store any digital data. Most PDAs run computer software, giving them many of the same capabilities as personal computers. For example, PDA users can work with word-processing documents, spreadsheets, and presentations. PDAs may also include global positioning system ("GPS") technology for determining the location of the device.

f. Tablet: A tablet is a mobile computer, typically larger than a phone yet smaller than a notebook, that is primarily operated by touching the screen. Tablets function as wireless communication devices and can be used to access the Internet through cellular networks, 802.11 "wi-fi" networks, or otherwise. Tablets typically contain programs called apps, which, like programs on a personal

computer, perform different functions and save data associated with those functions. Apps can, for example, permit accessing the Web, sending and receiving e-mail, and participating in Internet social networks.

g. Pager: A pager is a handheld wireless electronic device used to contact an individual through an alert, or a numeric or text message sent over a telecommunications network. Some pagers enable the user to send, as well as receive, text messages.

h. IP Address: An Internet Protocol address (or simply "IP address") is a unique numeric address used by computers on the Internet. An IP address is a series of four numbers, each in the range 0-255, separated by periods (e.g., 121.56.97.178). Every computer attached to the Internet computer must be assigned an IP address so that Internet traffic sent from and directed to that computer may be directed properly from its source to its destination. Most Internet service providers control a range of IP addresses. Some computers have static—that is, long-term—IP addresses, while other computers have dynamic—that is, frequently changed—IP addresses.

i. Internet: The Internet is a global network of computers and other electronic devices that communicate with each other. Due to the structure of the Internet, connections between devices on the Internet often cross state and international borders, even when the devices communicating with each other are in the same state.

21. Based on my training, experience, and research, I know that the Device has capabilities that allow it to serve as a wireless telephone, digital camera, portable media player, GPS navigation device, and PDA. In my training and experience, examining data stored on devices of this type can uncover, among other things, evidence that reveals or suggests who possessed or used the device.

ELECTRONIC STORAGE AND FORENSIC ANALYSIS

22. Based on my knowledge, training, and experience, I know that electronic devices can store information for long periods of time. Similarly, things that have been viewed via the Internet are typically stored for some period of time on the device. This information can sometimes be recovered with forensics tools.

23. *Forensic evidence.* As further described in Attachment B, this application seeks permission to locate not only electronically stored information that might serve as direct evidence of the crimes described on the warrant, but also forensic evidence that establishes how the Device was used, the purpose of its use, who used it, and when. There is probable cause to believe that this forensic electronic evidence might be on the Device because:

a. Data on the storage medium can provide evidence of a file that was once on the storage medium but has since been deleted or edited, or of a deleted portion of a file (such as a paragraph that has been deleted from a word processing file).

b. Forensic evidence on a device can also indicate who has used or controlled the device. This "user attribution" evidence is analogous to the search for "indicia of occupancy" while executing a search warrant at a residence.

c. A person with appropriate familiarity with how an electronic device works may, after examining this forensic evidence in its proper context, be able to draw conclusions about how electronic devices were used, the purpose of their use, who used them, and when.

d. The process of identifying the exact electronically stored information on a storage medium that is necessary to draw an accurate conclusion is a dynamic process. Electronic evidence is not always data that can be merely reviewed by a review team and passed along to investigators. Whether data stored on a computer is evidence may depend on other information stored on the computer and the application of knowledge about how a computer behaves. Therefore, contextual information necessary to understand other evidence also falls within the scope of the warrant.

e. Further, in finding evidence of how a device was used, the purpose of its use, who used it, and when, sometimes it is necessary to establish that a particular thing is not present on a storage medium.

24. *Nature of examination.* Based on the foregoing, and consistent with Rule 41(e)(2)(B), the warrant I am applying for would permit the examination of the Device consistent with the warrant. The examination may require authorities to employ techniques, including but not limited to computer-assisted scans of the entire medium, that might expose many parts of the device to human inspection in order to determine whether it is evidence described by the warrant.

25. *Manner of execution.* Because the warrant seeks permission to examine a device already in law enforcement's possession, the execution of the Device warrant does not involve the physical intrusion onto a premises. Consequently, I submit there is reasonable cause for the Court to authorize execution of the warrant at any time in the day or night.

CONCLUSION

26. I submit that this affidavit supports probable cause for a warrant to search a black Samsung cellular telephone, serial number IMEI No. 355357110651085 (the "Device") in law enforcement possession in an evidence locker at 600 Arch Street, Philadelphia, Pennsylvania, as further described in Attachment A, and the extraction from that property of electronically stored information described in Attachment B.

Respectfully submitted,

/s James Finnegan
JAMES FINNEGAN
Special Agent
Federal Bureau of Investigation

Subscribed and sworn to before me
on November 23, 2020:

/s Carol Sandra Moore Wells
HONORABLE CAROL SANDRA MOORE WELLS
United States Magistrate Judge

ATTACHMENT A

The property to be searched is a black Samsung Cellular Telephone, serial number IMEI No. 355357110651085 (the "Device"). The Device is currently in law enforcement possession at 600 Arch Street, Philadelphia, Pennsylvania.

This warrant authorizes the forensic examination of the Device for the purpose of identifying the electronically stored information described in Attachment B.

ATTACHMENT B

1. All records on the Device described in Attachment A that relate to violations of 18 U.S.C. § 2113(a) (bank robbery) and involve William Leinhauser a/k/a Trisha Moon, since July 17, 2020, including:

a. Planning of, commission of, flight from, or communications about robberies; the possession of firearms or ammunition; and the distribution, expenditure, or location of proceeds of robberies.

b. Photographs of: Leinhauser, victims, financial institutions, coconspirators / accomplices, clothing worn during the robberies, vehicles used during robberies, weapons, items used during the robberies, U.S. Currency, items purchased following robberies.

c. All information recording Leinhauser's schedule, travel, or location.

d. All bank records, checks, credit card bills, account information, and other financial records.

f. Address books and calendars.

g. All information regarding whether Leinhauser had the intent or scienter to commit the crime.

2. Evidence of user attribution showing who used or owned the device at the time the things described in this warrant were created, edited, or deleted, such as logs, phonebooks, saved usernames and passwords, documents, and browsing history.

As used above, the terms "records" and "information" include all of the foregoing items of evidence in whatever form and by whatever means they may have been created or stored, including any form of computer or electronic storage (such as flash memory or other media that

can store data) and any photographic form.

This warrant authorizes a review of electronic storage media and electronically stored information seized or copied pursuant to this warrant in order to locate evidence, fruits, and instrumentalities described in this warrant. The review of this electronic data may be conducted by any government personnel assisting in the investigation, who may include, in addition to law enforcement officers and agents, attorneys for the government, attorney support staff, and technical experts. Pursuant to this warrant, the FBI may deliver a complete copy of the seized or copied electronic data to the custody and control of attorneys for the government and their support staff for their independent review.